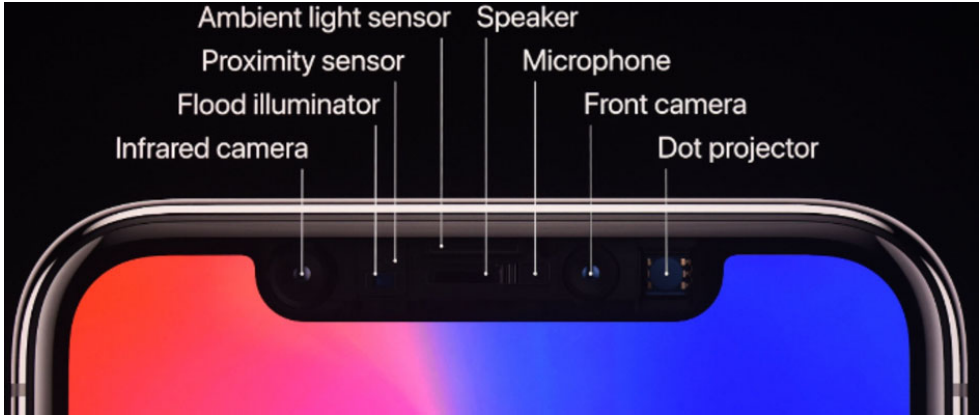# EXHIBIT F

Claim Chart for U.S. Patent No. 9,269,208 ("the '208 Patent")

The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone type cellular phones and Apple iPad type tablets, including the Apple iPhone X and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '208 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '208 Patent literally and, to the extent not literally, under the doctrine of equivalents.
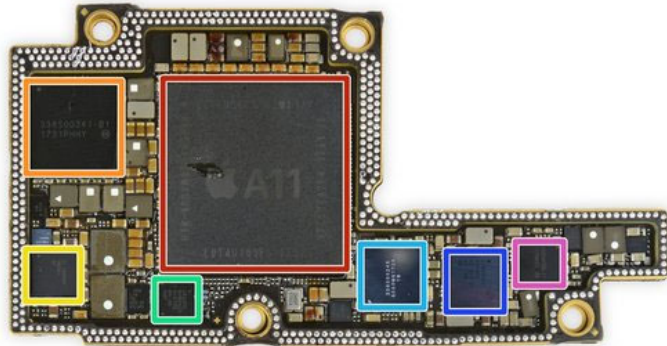
The products accused of infringing the '208 Patent include the Secure Access Accused Products equipped with Apple Card loaded into the iPhone Wallet ("the Secure Pay Accused Products").
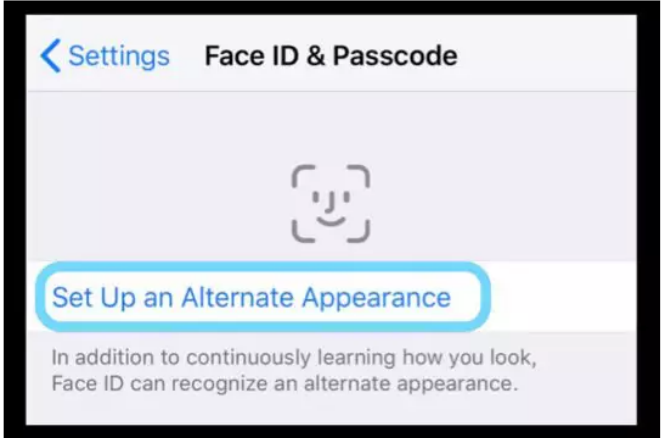
Claim 10	Apple iPhone X
10. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled	To the extent that the preamble is deemed to be a limitation, the Apple iPhone X is configured to use a system in accordance with this claim.

Claim 10	Apple iPhone X
item dependent upon information in said secure access signal, the method comprising the steps of:	
10a. populating the database of biometric signatures by: receiving a series of entries of the biometric signal;	**The Apple iPhone populates the database of biometric signatures by receiving a series of entries of the biometric signal.** More specifically, the Apple iPhone X has a secure enclave (SEP) in the A11 chip that populate the database of an encrypted mathematical representation of face images used for Face ID based on a series of face image received by TrueDepth camera system. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108

Claim 10	Apple iPhone X

https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975

https://www.phonearena.com/news/TrueDepth-camera-iPhone-X-Face-ID-Animoji_id108355 |

Claim 10	Apple iPhone X
	Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf

Claim 10	Apple iPhone X
	  ● Apple APL1W72 A11 Bionic SoC layered over SK Hynix H9HKNNNDBMAUUR 3 GB LPDDR4x RAM https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975

Claim 10	Apple iPhone X
	How-To Add Multiple Users to Face ID If you want to add a new user to Face ID on your iPhone, the steps are pretty straightforward. **Here is what you will need to do:** 1. Open **Settings** 2. Scroll and select **Face ID & Passcode** 3. Enter Passcode 4. Tap **Set up an Alternative Appearance** https://appletoolbox.com/multiple-face-id-users-ios-12/
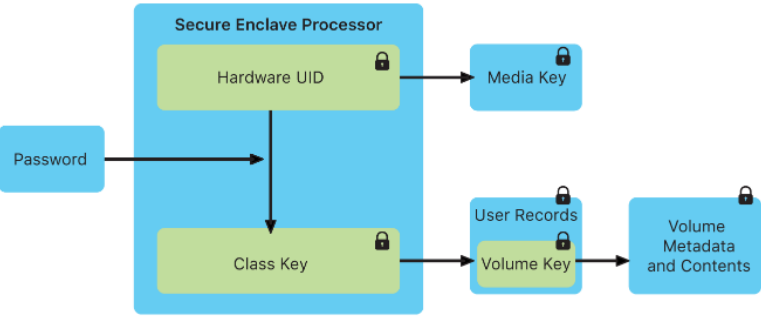
Claim 10	Apple iPhone X
	  https://support.apple.com/guide/iphone/set-up-face-id-iph6d162927a/ios
10a1. determining at least one of the number of said entries and a duration of each said entry;	**The Apple iPhone X populates the database of biometric signatures by determining at least one of the number of said entries and a duration of each said entry.** More specifically, the Apple iPhone X receives a series of face images through its image sensor on the TrueDepth camera system by having users move or tilt their head to set up a Face ID.

Claim 10	Apple iPhone X
	https://support.apple.com/en-us/HT208109
10a2. mapping said series into an instruction; and	**The Apple iPhone X populates the database of biometric signatures by mapping said series into an instruction.** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that can map biometric signals into an instruction. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data.

Claim 10	Apple iPhone X
	https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108
10a3. populating the database according to the instruction;	**The Apple iPhone X populates the database of biometric signatures according to the instruction.** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that can generate an authentication score based on its program instructions to determine whether the device can be unlocked. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108

Claim 10	Apple iPhone X
10b. receiving a biometric signal;	**The Apple iPhone X provide secure access to a device by receiving a face image.** More specifically, the iPhone X includes a secure enclave processor (SEP) that receives translated face images through an image sensor located on the camera to populate the database of face images. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108
10c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;	**The Apple iPhone X provide secure access to a device by matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that matches a face image against the enrolled facial image data and generate a matching score. The matching score generated by SEP is then transmitted to a processor. When the matching score is above the unlock threshold, the device can be unlocked.

Claim 10	Apple iPhone X
	Facial matching is performed within the secure enclave using neural networks trained specifically for that purpose. We developed the facial matching neural networks using over a billion images, including IR and depth images collected in studies conducted with the participants' informed consent. We worked with participants from around the world to include a representative group of people accounting for gender, age, ethnicity, and other factors. We augmented the studies as needed to provide a high degree of accuracy for a diverse range of users. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. An additional neural network that's trained to spot and resist spoofing defends against attempts to unlock your phone with photos or masks. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf a device-specific random pattern. A portion of the A11 Bionic processor's neural engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of your face captured across a variety of poses. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf
10d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	**The Apple iPhone X provide secure access to a device by emitting a secure access signal conveying information dependent upon said accessibility attribute** More specifically, the iPhone X includes a secure enclave processor (SEP) configured to deliver secure access signal to application processors. "SEP is involved in a facial recognition authentication process involving images captured by camera and processed by ISP. SEP may be a secure circuit configured to authenticate an active user (e.g., the user that is currently using device) as authorized to use device. A "secure circuit" may be a circuit that

Claim 10	Apple iPhone X
	protects an isolated, internal resource from being directly accessed by an external circuit." the '835 Publication, ¶¶048 The Secure Enclave also maintains the integrity of its cryptographic operations even if the device kernel has been compromised. Communication between the Secure Enclave and the application processor is tightly controlled by isolating it to an interrupt-driven mailbox and shared memory data buffers. The Secure Enclave processor. https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web
10e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	**The Apple iPhone X provides conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.** More specifically, the iPhone X includes a processor that controls the unlocking of the phone based on the matching score received from a secure enclave processor (SEP).

Claim 10	Apple iPhone X
	With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108